Could your Building Catch a Virus?  
Measuring the Impact of Cyber Security Threats on Building Management Systems  

K. Karagiannis¹, D. Chana², D. Fisk¹  
¹ Laing O’Rourke Centre for Systems Engineering & Innovation,  
Department of Civil and Environmental Engineering, Imperial College London, London, UK  
² Institute for Security Science and Technology, Imperial College London, London, UK  

ABSTRACT  
The close control of building services is seen as essential component for delivering low energy performance. This inevitably means some form of supervisory control and data acquisition (SCADA) system. To increase the penetration of this technology into the market place, it is inevitable that internet communication will be employed increasingly in the future. However, it can be very challenging to ensure that a widely dispersed monitoring network is secure from cyber attacks. Tools are readily available on the Web that can challenge the Building Management Systems (BMS), especially if they are not configured carefully. The nature of these threats is explained. Results are reported using the search engine Shodan. This search engine was able to find the IP address of a controller several thousand miles away through the internet that had been purposefully misconfigured. It is concluded that ensuring a secure system will be a critical component of commissioning any new advanced Building Energy Management system. Without this step the application of intelligent building technology designed to meet challenging energy performance will be limited to low profile projects. In the near future, when BMSs will be integrated into the Smart Grid, poor cyber security of building management systems will pose a threat not only to the building itself, but to a country’s infrastructure as well.

INTRODUCTION  
The imperative to improve energy performance has imported into building services SCADA systems technology from industry. Industrial control systems are frequently configured to hold flows at optima values. While these flows may be at impressive pressures, arguably building controls have a hard task because heating and cooling loads are continually changing. There is always a risk that poor control leads to heating and cooling plant fighting each other to service some zones. Intelligent buildings frequently deploy active solar control, occupancy sensing, lighting control, as well as being able to change the season mode of operation of the building. It is difficult to see how advanced buildings can achieve their design expectations without close monitoring and control. Failure to ensure that the systems are cyber secure may risk the whole application of this exciting technology. Whole systems solutions for other low energy technology such as passive cooling or solar panels naturally include restraints relating to the physical security of a building. That is rational because one of the primary purposes of a structure is to keep its occupants ‘safe’. What has not been widely recognised is that comparable constraints apply to BEMS. Part of the responsibility for cyber security lies with the client, to make sure that enterprise’s general security standards are met.

Cyber security has not been an issue previously considered for Operational Technology, especially in the design phase. As the systems in OT move from ICS (Industrial Control Systems) to CPS (Cyber-Physical Systems) and to the IoT
(Internet of Things), many questions arise regarding the security and robustness of these systems. Stuxnet, a computer worm back in 2010 that targeted the PLCs (Programme Logic Controllers) of an Iranian Nuclear Plant hit the media and drew attention concerning cyber security in ICS. Since then, there is a sharp increase in incidents about cyber-attacks in ICS and cyber security awareness has been raised not only, for control systems in critical environments, but for Building Management Systems as well.

Building Management Systems (BMS) aim at managing and controlling the mechanical and electrical equipment of a building and its' subsystems through integration. Following other SCADA (Supervisory Control and Data Acquisition) systems in the past, they used to be physically isolated and they constituted a separate network inside the building, using proprietary protocols and software. However, whilst “security through obscurity” has been a way to safeguard the BMS by using proprietary architecture this cannot be the case in modern control systems. The modern building environment requests current IT technology in order to improve and maintain the quality of building services and the effective operation of the systems associated with them. Since the trend for the modern BMS as it moves from the field level more to the management level, is to act as an umbrella for the different subsystems integrated into it, the continuous adoption of open standards and commercial off-the-shelf products is inevitable in order to achieve interoperability and flexibility. On the other hand, the BMS industry has not taken into serious consideration the security issues that arise from this modernization and it was not until recently that security breach occurred and signs of counter measures from the industry begin to show.

BACKGROUND

ICS is a wide-ranging expression that refers to different types of control systems with three main categories SCADA systems (Supervisory Control and Data Acquisition), DCS (Distributed Control Systems) and a hybrid of the two. (NIST SP 800-82-R, 2014)

- **SCADA**: systems that are implemented for data acquisition and control on dispersed geographical sites in large distances. The data collection from the field level is forwarded to a central computer facility where the information is visualized in graphical or text form, allowing an operator to monitor and control systems in different locations from a central point, simultaneously. SCADA systems are used in power transmission and distribution, oil and natural gas pipelines, water distribution, and transport systems. (NIST SP 800-82-R, 2014)
- **DCS**: systems used in sites located in the same neighbourhood, especially for process control in production. The control is achieved by a central control point supervising a set of subsystems in a lower level that direct a localized process. Distributed controllers manage processes through feedback or feedforward control while process variables remain at the desired level. DCS are mainly employed in power generation, wastewater treatment, oil refineries, chemical processes and the automotive industry. (NIST SP 800-82-R, 2014)

In practice, many of the ICS implemented, are a hybrid of both systems, since customisation in order to address the customers’ needs is usually required. Additionally, modern control system components allow integration on a level where SCADA and DCS may be combined, depending on the application.

BMSs can be categorized more as DCSs, since they are more based on distributed architecture in a single geographic location. However, nowadays in many cases a BMS can have SCADA features on the management level, supervising a range of BMSs in different locations through a WAN (Wide Area Network). Building Automation and Control has been a parallel industry with the Industrial Control Systems throughout the years. Although, as systems follow overall the same logic and present many similarities, there are a few significant differences between the two systems. BMSs mostly use DDC (Direct Digital Control) as control system components and hardly PLCs. DDC controllers differ from PLCs because they are designed especially for HVAC and lighting control applications in buildings and not for industrial and critical environments, where customization is first priority in comparison to cost. BMS controllers are pre-engineered and
preconfigured in order to achieve cost reduction and execute less complex functions that building services require. Likewise, programming, commissioning and maintenance of the system can be completed in a shorter period of time and demand less skilled technical staff for this purpose than a highly skilled PLC engineer. In addition to that, BMSs use different standards and protocols, especially designed for building automation (ex. BACnet), where high-bandwidth and low-latency are not as crucial as in critical and industrial environments. On the other hand, some BMS vendors manufacture controllers based on PLCs and use industrial protocols as CAN-bus for instance, that can be found in the automotive industry. Other industrial protocols implemented in Building Automation are Modbus and Profibus to name a few. BMSs are designed to be easy to configure, space and cost efficient and incorporate energy management functions that are not requested in industrial control systems yet.

Whilst BMS moves forward to the “internet of things” and integration will be realised at its highest level, cyber security has been considerably neglected by the industry. Cyber security measures have not been adopted in existing systems and recent reports about cyber incidents and events in BMS, support this notion. Although, the amount of cyber incidents that occurred specifically in BMSs have not yet been recorded by an established organisation or professional body, some cyber incidents are classified into the general category of ICS cyber incidents and events.

According to the U.S. Computer Emergency Readiness Team (CERT), there is a dramatic increase of 782% cyber incidents, reported from 2006 to 2012 (Fernandez Ivan, 2013). In 2013, ICS-CERT released a report stating that there have been 256 cyber incidents responded, with the majority of them regarding industrial control systems involved in critical infrastructure. More specifically, 59% present of the cyber incidents came from the energy sector and 20% from critical manufacturing. (ICS-CERT, 2013)

BMS cyber incidents are classified under the umbrella of ICS incident reports, thus there is no official recorded number of exclusive BMS cyber incidents and events. In addition, many incidents may remain unreported in order to avoid public disclosure and brand image erosion. In other cases, many incidents and events remain undetected from the asset owners, due to lack of auditing and intrusion detection tools. However, some BMS cyber incidents and events have been publicly reported which indicates the vulnerabilities of the existing systems and the need for prompt reaction to future cyber attacks. Some officially reported BMS cyber incidents and examples of potential damage are:

**The Carrell Clinic 2009:** A leader of a hacker group gained unauthorised access to the hospital’s HVAC control system. He posted images on the internet that presented the control interface of an HVAC plant that was responsible for the air-conditioning of the hospital’s surgery unit. The test alarm notification of the control system was turned to inactive. (Goodin Dan, 2009)

**Super Bowl XLVII Blackout 2012:** In 2012, a power outage lasting for 22 minutes stopped the game for 34 minutes due to a mechanical failure of a relay device. Although, this incident did not involve a cyber attack, cyber security experts consider this event as what could happen if the BMS that controls lighting in a stadium, fall into the hands of a potential attacker. (Korber Sabrina, 2013)

**US Business 1 2012:** as stated in the FBI report in 2012, intruders gained unauthorised access to the ICS network of the air-conditioning company US Business 1 in New Jersey. The ICS was using the Tridium Niagara ICS system that is widely known for vulnerabilities allowing remote management of the system. Through the ICS network they also gained access to the HVAC control system of the company. (FBI, 2012)

**Google Wharf 7 Building 2013:** In 2013, during a research project, cyber security researchers from Cylance gained access to the BMS of Google’s Wharf 7 Building in Australia. They posted screenshots of the BMS user interface showing floor plans, water and HVAC systems of the building. Though, they did not try to control the system and notified Google immediately for this vulnerability, they later stated that “If Google can fall victim to an ICS attack, anyone can”. (Rios Billy,
North Shore Private Hospital 2013: In the same research project from Cylance the two cyber security researchers discovered that the BMS of the North Shore Private Hospital in Sydney was protected by the user name "admin" and password "anyonesguess". This could allow possible attackers to easily hack into the system which was exposed to the internet, due to a weak password policy. (Grubb Ben, 2013)

Target 2014: In the Target incident earlier this year, phishers got access to the enterprise network of Target and stole card credentials of millions of customers. Although, there is no official evidence so far, experts believe that this security breach was achieved through the HVAC control and monitoring system that was remotely managed by a third-party vendor. (Krebs Brian, 2014)

IDENTIFICATION OF THREATS AND VULNERABILITIES

Security analysis for the system can be summarized in the following words; threats, vulnerabilities, risks, assets. Threat agents exploit known or unknown vulnerabilities of the system to damage assets and create risk to asset owners. The concept can be depicted in the following diagrams from the international standard ISO/IEC 15408-1 that describes the relationship between the different elements of security.

![Security Elements relationship (ISA-62443-1-1, 2013)](image)

Threat-Risk assessment shows how assets are subject to risks by various vulnerabilities that are exploited from threat agents and how risk can be minimized by adopting countermeasures.
In order to adopt countermeasures, first threats and vulnerabilities must be identified in current BMSs and then a risk assessment must be generated. BMSs are the asset in this case, as well as the building itself and its’ systems that are interconnected to the BMS, which can be put in jeopardy from cyber-attacks. In many cases, the main target for the attackers may not be the building’s BMS, but other systems like the enterprise network that through the BMS it can be reached for malicious attacks.

**Threats**

The ISO/IEC FIDIS 27005:2008 defines threat as any potential cause of incident that can have negative consequences in a system or an organization. Threats are related to other terms as threat source and threat event or incident. Threat source is addressed to the intent or method that threats have to exploit vulnerabilities. A threat event is an event that is likely to have a negative impact on a system or organization, whereas an incident is when the event actually occurs. Threat sources can be divided into internal or external.

Internal threat sources may be threat agents that have physical access to the system components or authorised network access to the system from the inside of the security perimeter and often called insiders. The knowledge of hacking in this case is not a prerequisite since insiders usually have physical access to the BMS system components, such as control panels or control rooms usually left unlocked and can penetrate to the system’s network without having first to break the security defences, if any exist. From there, they can for instance, insert a USB device that contains malicious software into a controller or the central computer that usually runs on commercial operating systems’ platforms. Added to this, they can also remain untraceable due to the common use of usernames such as “administrator”, “operator” and “user” to access system components. Moreover, privileged users that obtain authorised network access to the system, do not only need to have physical access to the system components to cause problems. A modern IP enabled Building controller with an embedded web - server can easily accessed from anywhere through the internet and inflict harm based on the attacker’s incentives.

External threat sources are threat agents that have no physical access or authorised network access to the system and
need to hack the system defences for penetrating into it and cause damage. However, in cases where a security perimeter for the BMS is not defined and an attacker can obtain authorised access to a web-embedded controller through the internet using default usernames and passwords published often on the internet by the vendor, can also be classified as an external threat.

The main external threat to the BMS is the internet. Potential attackers will use the internet to intrude into the BMS network, either because they want to compromise the system itself or to use the BMS as a “back-door” to reach another network connected to it (ex. Enterprise network). Furthermore, the use type of building plays a major role to motivate attackers to break into the BMS network. Military facilities, for example, may have high-level security when it comes to physical access, but the BMS that controls the premises’ mechanical and electrical equipment may not be safeguarded as it should. For an intentional attacker the BMS network acts as the vulnerable access point to reach his target.

Vulnerabilities

System vulnerabilities can be defined as weaknesses of the system in security issues related to policy and procedures, hardware and software of system components, system’s architecture and communication networks. Vulnerabilities are the holes of the system that allow threat sources to exploit them in order to jeopardise the BMS or use them as a “back-door” to other systems interconnected to the BMS. Owing to the large variety of building types that the BMS can be implemented and the multiple vendors of the system components, BMSs may differ considerably depending on the plant equipment they control, the communication protocol they use, the systems integrated into it, the system’s architecture as well as on the security policy applied by the building owner. Thus, vulnerabilities cannot be determined clearly, unless these features are defined and identified in detail. However, some common vulnerabilities are frequently discovered in current BMSs, especially nowadays that the use of commercial-off-the-shelf products is increasing dramatically in the BMS industry. Overall, BMSs’ vulnerabilities can be divided in policy and procedure, hardware, software, network and communications as well as configuration.

Security policy in building automation has never been a major concern for the industry until recently, when certain cyber incidents occurred. Certainly, security and safety in the design of system components regarding environmental conditions such as temperature, humidity and explosive environments were seriously considered but the security of the whole system in operation was significantly neglected. Whilst the primary BMS was designed like other ICSs as an isolated system, systems started to become more complex and interoperability as well as system integration, were an immediate request from the market. Nevertheless, BMSs may moved in this direction, but a security policy for the new features was not introduced from the industry. Consequently, this mentality was inherited also to the system integrators, operators, and maintenance and facility management staff. Security policy in organizations may be implemented when it comes to IT networks and equipment, but building control systems are usually ignored due to lack of knowledge and unknown communication capabilities of the systems or because no one informed them about security issues. Policy and procedure are one of the main significant vulnerabilities of the BMS since it is a matter of coordination between the BMS manufacturer, the installer, the operator and the asset owner. The first part of the chain provokes the next so that a security policy may be defined and implemented. In many cases, especially in legacy systems, technical documentation and specifications of the system are poor or they do not even exist. Many organizations are not fully aware of their complete BMS architecture or the full range of system components that are in operation or have been replaced. In legacy systems, many functions of the BMS may have been disabled or system components like a controller or a thermostat may have been replaced without being properly commissioned. New systems may have been integrated or older systems may have been disconnected. A system that is not completely known it is impossible to be safeguarded effectively. In such cases, retro-commissioning is a prerequisite for security procedures to be implemented.

BMSs include system components that are designed for a wide range of functions and due to flexibility and cost reduction some of them can also have multiple uses as standalone controllers, as sensors and actuators for smaller
applications or can be integrated into third-party systems. Thus, this makes the hardware of the system vulnerable since the customisation of the system is based on the system designer that may use different components from multiple vectors. Although, the system components individually may have been tested for security issues, the final BMS system will be actually tested in live operation. Thus, if the hardware of the system contains design flaws that have not been detected before, security problems may arise.

Software is an integral part of the BMS to execute control functions and can be found at all levels of the system, field, automation and management level. Smart sensors and actuators, controllers and central computers all include software that may have unknown vulnerabilities. Frequently, software contains design flaws that until a security breach or a malfunction occurs, they remain unknown. In such cases, vendors release software patches that must be installed immediately to fix the problem and secure the system. However, especially in legacy building automation systems and systems that are not connected to the internet or the vendor's server, software updates must be installed manually and it depends on the system operator or maintenance department to do so. Regularly, vendors use third-party software in many system components that may contain vulnerabilities that they are not fully aware of and they may not be able to fix promptly in case of an attack. This software may come from a single manufacturer and may be applied in different types of applications in ICS, as SCADA and DCS. Consequently, an exploitable vulnerability found, for instance, in an industrial SCADA system can affect a wide range of devices from different vendors in the BMS industry.

The network architecture of a BMS is a critical part concerning cyber security, since it is through the communication network that most cyber-attacks will be performed. Unfortunately, BMS networks are often not taken into serious consideration in the design phase or change in the implementation phase from the initial design. In many cases, one of the main issues is that the asset owner has not clear view of the complete system architecture or of the connection links with other systems. BMSs may allow remote access for remote control and monitoring, but they should always be kept inside security defences. Proprietary protocols may have been the common practice in the past defending the network by “security through obscurity”, but as the industry adopts open protocols and standards, the vulnerabilities increase in the communication layer. However, this does not mean that proprietary protocols are the answer, as many vulnerabilities have been reported in conferences regarding them and they cannot be tested properly due to lack of expensive equipment and facilities from vendors. BMS components are becoming IP-enabled and integrate IT technology that oppose a risk if security measures are not implemented correctly.

As already mentioned, BMSs are unique systems due to diversity of various system components from different vendors that constitute the system. Vendors may have included security features in their products, but this does not mean that security is inherited in the whole system. Hence, it is upon the system installer to configure the system correctly and ensure security as well as the system operator to maintain configuration at an acceptable security level. Most of the deficiencies that have to do with configuration in BMSs are the low level of authentication and access. The use of default passwords in accessing web-enabled automation controllers or central control PCs is very common in BMSs. Default passwords can be found easily in technical manuals published on the manufacturer’s website or on websites listing devices and their default passwords. Default passwords may have not been changed due to lack of password policy within the organisation. Furthermore, even if the password is changed usually remains weak and lockout policy as well as password history is not enabled. Short passwords or easily guessed ones, can be hacked with spending less time and resources by potential attackers. Strong, long and complex passwords must be applied in BMS components to prevent unauthorised access.

**SHODAN**

Shodan is a computer search engine launched in 2009 by John Matherly that identifies specific computer devices connected to the internet like servers, routers, industrial controllers etc. The user can make queries online for certain terms through a web-interface. Shodan can find IP-enabled devices as webcams, printers and heating systems that are connected
to the internet and display specific information about them, like firmware version, location, and IP address. Therefore, Shodan is often called the “Google for hackers” or the “search engine for the Internet of Things”. Nevertheless, Shodan differs from Google engines like Google and Bing since it does not search for context on web pages, but it interrogates ports to receive the returning banners. Banners can be defined as metadata that the client receives from the server (Matherly J, 2014).

In the popular searches section of Shodan, the term “webcam” is the first listed with 4,083 queries. IP-enabled video cameras have been deployed the recent years, allowing surveillance remotely through the internet. IP cameras are part of the CCTV (Closed Circuit Television) system that in large buildings it is usually integrated into the BMS along with the Access control system. IP cameras can send information to the BMS regarding the occupancy level of a space in order the BMS to adjust the HVAC or lighting control accordingly. From this, derives that if hackers are pointing to CCTV systems to attack, through interconnectivity BMSs are also affected.

Fifth in the list of popular searches is the term “default password” with 433 searches. This query presents results where the “default password” is included in the banner. Surprisingly, many banners contain what the default password actually is. In one case, the username was “admin” and the password was “password”. Certainly, this does not mean that the device can be accessed by these credentials. However, the possibility still remains, considering the use of weak passwords in BMSs mentioned in Vulnerabilities section.

**LIVE EXAMPLE**

In an attempt to show that BMSs are vulnerable to cyber-attacks a live example is demonstrated for this purpose. With the assistance of Shodan it was possible to identify exposed BMS components on the internet. After the initial search of general terms concerning BMSs, a query for a specific model of Building Automation controller was performed. The next step was to connect a dummy controller of this type on the internet. The controller was easily accessed from a remote location several thousand miles away through the internet and it was available for monitoring and configuration. Finally, the last step of the experiment was to identify if the specific controller would be scanned from the Shodan search engine.

The first search term inserted in Shodan search engine was the general term “BMS”. The number of results displayed concerning this term was 1,054. However, this does not prove that all 1,054 are Building Management System devices, since the term “BMS” in the banner may refer to something else. In one case, the term BMS in the banner was part of the brand name of a consulting group. On the other hand, a banner message from a server in Russia was containing the phrase “Servername: BMS-SERVER” running on Microsoft Windows that seems likely to be the main control server of a building automation system installed in a building, located in Russia. Moreover, phrases like “BMS-PC” and “BMS-SERVER” in the server name were found multiple times. In one case, the server name in the banner message was the name of a popular building management software followed by the word BMS. This made clear that it was the server of a Building Management System with this software installed. Finally, the most representative example of the results for building automation systems was the identification of multiple Bacnet devices from a building in Australia. After searching on the internet the Model and Vendor's Name, included in the banner, it was found that is a Bacnet/IP controller for HVAC equipment. Bacnet communication protocol was created by ASHRAE especially for Building Automation. Conclusively, the next step was to use as query the term “Bacnet” and port:47808 that the Bacnet communication protocol uses as default, in order the search to be narrowed only into Bacnet devices.

The search identified 5,534 Bacnet devices in Shodan with 3,650 of them located in the United States. The second country in the list was Canada with 685 devices. Despite this, the map generated by Shodan indicated that Bacnet devices were discovered globally, excluding mostly Africa and some part of South America. Shodan also displays the ISP (Internet Service Provider) of the device detected and the domain information if it is available. In some cases that the ISP is not a telecommunication company, the name of the organization that the device is located can be recognised. In this specific search among others, many academic institutions were identified in the United States, Spain, France, Australia and the
A specific model type of a Bacnet/IP controller used in BMSs named X was chosen from the manufacturer Y for the next query in Shodan. Manufacturer Y is specialised in building automation control with a long history in the building control sector. The model X is a programmable DDC controller that enables Bacnet/IP communication according to EN ISO 16484-5, and uses an embedded web-server for remote access. Additionally, it can be implemented as a standalone controller or as a part of a BMS network for controlling and monitoring mechanical and electrical equipment. The controller has integrated functions such as time schedules, calendar, data and alarm historian.

In Shodan the model type of controller X was inserted in the search engine and 208 results were returned. All the results were related to the specific controller with France and Spain being the top locations for this model type. Unfortunately, the domain information did not reveal in most cases the type of buildings that the controllers are located, except ISP names. Still, in 12 cases the domain name was an academic institution in Spain and one in Germany. Specific dates were added to the next searches in Shodan showing that all controllers were added in the Shodan database in 2014. More specifically, in a time period of three months, 123 controllers were launched on the internet indicating a sharp increase of approximately 59%. The banner of controller X in Shodan reveals significant information about the device. The information revealed depends on the configuration that was made in the device by the programmer of the controller.

For example, in a banner returned from the Bacnet controller X, part of a BMS installed in a hotel in Spain, the following information was provided:

- The Instance ID that reveals the unique device ID in the network. The Vendor ID that shows the name of the manufacturer Y. The model name field that is the type of model of the device, in this case was X. Other fields displayed the current versions of firmware and software while in the location field, the name of the hotel was disclosed. In the description field, the name of the hotel was repeated, followed by the public IP of the device and the internal IP in the local network.

Furthermore, in many instances of this query, the Object name indicated the plant assigned to the controller together with the number of the automation station in the network.

A potential attacker gaining access to this information can easily compromise the system. Looking to the current version of firmware and software, he can find on the manufacturer’s Y website if these are the latest versions installed. If a known vulnerability is released on the manufacturer’s website and the device has an earlier version, then the attacker can exploit this published vulnerability for his own benefit. Furthermore, the public IP address given from Shodan will allow the attacker to access the web-server of the controller from the internet. If the default username and password has not been changed, then the attacker can gain authorised access to controller X by using the default password available on the manufacturer’s Y website. In this case, the default password gives the attacker administrator’s privileges that can be used to configure the controller X and modify data and settings.

In order to assess the capability of Shodan to identify BMS devices connected to the internet and how vulnerabilities can be exploited by potential adversaries, a controller X was connected to the internet for this purpose. The controller X did not control any real plant equipment, but it was programmed with specific functions for HVAC equipment. Controller X was configured with a software tool in order to allow communication with the Bacnet/IP network. The router’s firewall was disabled to allow requested ports to operate. A public IP was assigned to controller X and was tested if it was accessible through the internet. The author accessed the web-interface of the controller by inserting the assigned IP address to a web browser.

After the successful launch of the controller X on the internet, a search was performed in Shodan. The search term included the controller’s X model type followed by the filter of country in which the controller X was located. The controller X was identified by Shodan search engine after 14 days. The information in Shodan disclosed the ISP name, controller’s X public IP and geolocation, vendor’s ID, application software version, firmware version, device ID, model name and the plant equipment the controller is assigned to control in the description field. However, even after controller X was disconnected from the internet, it still showed up in Shodan searches.
DISCUSSION

The research in literature concerning BMSs has shown that there is no clear classification of BMSs as ICSs. In many cases, BMSs are considered to be a sub-category of ICSs, where BMSs in truth are a parallel industry with ICSs and present a few key differences. ICSs are mainly implemented to control and monitor critical infrastructure and industrial processes, in contrast to BMSs that are installed only in the building environment. Buildings are not regarded as critical environments, nor require the accuracy and safety of industrial processes. Building automation aims to improve living conditions inside the building environment, ensure safety and increase the energy efficiency of the building. On the other hand, in ICSs time is critical and system failure can have severe consequences. Until now, energy saving is not a priority in industrial environments. As mentioned before, the system components used in BMSs differ in some parts from ICSs in design, functionality and applicability.

Due to these diversities BMSs should follow separate guidelines when it comes to cyber security. Nevertheless, there is no clear distinction between BMSs and ICSs in cyber security literature. Possibly, this is because the literature in BMSs can be characterised as poor, in general. Explanation on this matter may be that building automation industry was not an open industry until recently. Owing to the fact that most of the BMSs were proprietary systems certain rights should be purchased to publish books about building automation. Most of the older books in literature analyse proprietary systems or protocols and it wasn’t until recently that open protocols and systems were discussed.

This ambiguity in literature about BMS’s classification and the lack of tailored guidelines can be considered as vulnerability with reference to cyber security. If there is not enough documentation to support the BMS stakeholders from the system integrator to the asset owner, then security policies and procedures cannot be implemented effectively.

The results of the case study in Shodan indicated that a considerable number of BMS devices are exposed to the internet. The fact that the IP addresses of these devices are saved in the Shodan database means that there are not behind a firewall and a security perimeter is not defined. Some of the buildings identified, are large complex buildings like Universities and hotels that can be easy targets for cyber attackers. The ability of Shodan to detect BMS devices and reveal available information as geolocation, software version and vendor’s id, is a useful tool for penetration testing, whilst a dangerous tool for potential attackers. It can be similar to a thief that knows that one back door or window in a house is open but he has to search to find out which one, in order to get in. However, Shodan does not reveal information that is not already there and is a good reason for the industry to start adopting cyber security measures.

On the other hand, the fact that controller X was identified by Shodan after 14 days of its’ initial launch on the internet, proves that the data in Shodan are not real-time data. Moreover, even after controller X was disconnected from the internet, it still showed up in Shodan searches. This is explained from the fact that Shodan uses a web crawler that scans the internet regularly for IP addresses and saves the returned banners in a database. According to a research study that assessed the ability of Shodan to identify PLCs connected to the internet, Shodan randomly selects IP addresses and then randomly interrogates ports. (Bodenheim, R. et al, 2014). As a result, if Shodan has never visited the desired network, it will not index the device requested. In the same study, the devices used for the assessment were scanned successfully and indexed by Shodan within 19 days. Conclusively, the fact that BMS devices are identified and listed in Shodan does not mean that they are still exposed to the internet, but at some point in the past they were. Another aspect is that a larger number of BMS devices may be exposed to the internet that Shodan have not indexed yet.

Another question that emerges from the above analysis is, if current IT solutions are enough to safeguard the system. Although the convergence between OT and IT is a fact nowadays, BMSs present considerable differences in comparison to IT. Firstly, the BMSs are designed for a lifetime of almost 10 years and many legacy systems have served buildings for a longer time. On the contrary, IT systems have a shorter lifetime and are replaced regularly every 3 to 5 years. Secondly, in IT confidentiality of data is the first priority, followed by integrity and availability, whereas in BMSs availability is the main concern. Interruptions in IT systems may not have severe consequences for the organisation, whilst in BMSs uninterrupted operation is normally required. Moreover, time delays in IT systems are often acceptable in comparison with building
automation that immediate response is of paramount importance, including critical alarms and emergency mechanisms triggered by fire safety systems, for instance. Last but not least, information management is completely different from control of mechanical and electrical equipment. Typically, control systems are more complex than IT and can generate unexpected effects, in case of failure, difficult to be managed by IT personnel. In order for the BMS to be defended properly, it requires not only deep knowledge of the system itself, but of the equipment that controls and of the systems that interacts with.

CONCLUSIONS

BMS is an integral part of the low energy future. But whereas security would be an integral part of other design options such as passive ventilation or the external mounting of expensive solar panels, it has not to date featured in BMS configuration. The integral part of cyber security in Building Management Systems is neglected significantly by the industry. However, as buildings become more intelligent and integration is requested at a higher level, Building Management Systems become more complex and sophisticated. The continuous incorporation of commercial-off-the-shelf products has resulted in increasing the vulnerabilities in BMSs. Even where the manufacturer has taken security into consideration, this research has exposed that proper security commissioning is necessary. This is no mean task as it involves the set-up of many geographically spread objects sometimes in a legacy system of ill-defined architecture. At least one Code of Practice has been recently issued for cyber security in the built environment, and this is likely to be a growing trend if BMS are to be widely deployed.

Finally, there is a potential market for commercialisation of the cyber security assessment of BMSs. The lack of cyber security experts that have deep knowledge of the system constitutes an opportunity for market establishment. Currently, cyber security in BMSs is performed by IT consultants that make use of IT products to safeguard the system. Although, IT solutions can improve the security of a BMS, a defence-in-depth strategy requires the involvement of a BMS cyber security expert that will act as the bridge between Operation and Information Technology.

REFERENCES


Leverett E., 2011. Quantitatively assessing and visualizing industrial system attack surfaces (M.Phil. Dissertation), Darwin College Computer Laboratory, University of Cambridge, Cambridge, United Kingdom.


NIST SP 800-82-R1. 2013. Guide to industrial control systems (ICS) security. National Institute of Standards and Technology Special Publication, Special Publication 800-82, Revision 1


